College of Healthcare Information Management Executives

Acting Secretary April Tabor
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

Submitted via Regulations.gov

Acting Secretary Tabor,

The College of Healthcare Information Management Executives (CHIME) welcomes and thanks you for the opportunity to comment on the *Health Breach Notification Regulatory Review; request for public comment* published in the Federal Register on May 22, 2020.

CHIME is an executive organization dedicated to serving chief information officers (CIOs), chief medical information officers (CMIOs), chief nursing information officers (CNIOs) and other senior healthcare IT leaders. With nearly 3,400 members, CHIME provides a highly interactive, trusted environment enabling senior professional and industry leaders to collaborate; exchange best practices; address professional development needs; and advocate for the effective use of information management to improve the health and healthcare in the communities they serve.

The Federal Trade Commission (FTC) released the initial Breach Notification Final Rule in 2009 and since then much has changed in the health technology world. Health data is now an even more valuable commodity and mobile applications that use this data are growing in use. In addition, the U.S. government has begun to embrace the new health data economy with the release of two regulations from the Centers for Medicare and Medicaid Services (CMS) and Office of the National Coordinator for Health Information Technology (ONC) geared at unlocking a consumer's – and a company's – access to individual health data. With these major shifts in the health data landscape, it is clear the FTC's Breach Notification Rule (the Rule) must be updated to bring privacy and security policy into alignment with other initiatives happening nationwide.

To bring the Rule into alignment with other government initiatives, CHIME proposes the definition of who is required to comply with the Rule be augmented to go beyond just including personal health records (PHR), vendors of PHRs and PHR-related entities to any non-HIPAA covered entity that handles electronic health information (EHI) as defined by ONC. This change will better protect consumers and their health data privacy, and as discussed in our below responses to your questions, will strengthen the FTC's ability to enforce the Rule and ensure the health data ecosystem remains trusted and sound.

Breach notification requirements are critical in allowing consumers to react to a loss of their personal data, but they do not go far enough in working to prevent the breaches. There is more that can be done before the breach happens and we encourage the FTC to work with Congressional stakeholders and other federal agencies to expand the agency's ability to enforce real-world and stringent privacy and security protections on technology companies to better protect consumer data. That includes making sure consumers understand what they are agreeing to prior to using a company's technology. The

FTC's previously released mobile app development best practices[1] are a great starting point for many companies, but a lack of enforcement actions related to them allow companies to continually leave consumers behind in the development of their privacy policies. A New York Times privacy project found that of the 150 privacy policies they reviewed, most exceeded a high school, college, or professional career reading level[2]. These non-sensical privacy policies often leave consumers unaware of what they are agreeing to, often exposing their data to risky actors such as was the case with some Huawei created products[3]. Broadening the breach notification requirements under this Rule helps fill part of the new consumer protection void and are crucial to improving the security of patient health data, but more needs to be done to protect consumers before a breach event happens.

General Issues

1. Is there a continuing need for specific provisions of the Rule? Why or why not?

   Comment: CHIME is fully supportive of the continued use of the breach notification rule. Health data is becoming increasingly more valuable to hackers, with some experts believing it is now up to 10 times more valuable than credit card information.[4] In addition, commercializing health technology has also created an infinitely larger economic sector. Every year more and more private companies attempt to join the medical marketplace that are not traditional holders of medical data. That means companies previously focused on product streams dealing with mobile consumer applications and consumer technology are now capturing and holding consumer health information, yet they remain outside the purview of the Health Insurance Portability and Accountability Act (HIPAA). With this in mind, it remains crucial that requirements remain in place to police these non-HIPAA actors.

   There are significant changes that need to be made to the definition of who is covered by the FTC's rule. The Rule identifies covered parties subject to breach notification requirements as "vendors of personal health records (PHR) and PHR-related entities (i.e., companies that offer products and services through PHR websites or access information in or send information to PHRs)[5]." When the initial breach notification rule was released, the health information and technology landscape was not as complicated as the one we live in now. Health information is no longer secluded solely in PHRs. Electronic health record (EHR) use is now nearly ubiquitous across providers and the U.S. government has begun capitalizing on this large install base by recently finalizing two rules through CMS[6] and ONC[7], mandating the use of application programming interfaces (APIs) along with several other requirements designed to give patients more control of their health data. Within both of those regulations, the information that is deemed under their purview falls under the term "electronic health information (EHI)." For the first two years of the regulations' effective date – until May 2, 2022 – EHI is defined as the U.S. Core Dataset for Interoperability (USCDI)[8] and thereafter shifts to all electronic Personal Health Information (ePHI).

---

[1] https://www.ftc.gov/tips-advice/business-center/guidance/mobile-health-app-developers-ftc-best-practices
[2] https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html
[3] https://www.forbes.com/sites/kateoflahertyuk/2019/02/26/huawei-security-scandal-everything-you-need-to-know/#36f3906773a5
[4] https://www.beckershospitalreview.com/healthcare-information-technology/medical-records-10x-more-valuable-to-hackers-than-credit-card-information.html
[5] https://www.govinfo.gov/content/pkg/FR-2020-05-22/pdf/2020-10263.pdf pg. 31085, column 3, line 6
[6] https://www.cms.gov/newsroom/fact-sheets/interoperability-and-patient-access-fact-sheet
[7] https://www.healthit.gov/cures/sites/default/files/cures/2020-03/TheONCCuresActFinalRule.pdf
[8] https://www.healthit.gov/isa/united-states-core-data-interoperability-uscdi

We recommend the FTC modify its definition of who is covered under this rule from vendors of PHRs and PHR-related entities to include companies and entities that interact with and/or store electronic health information (EHI) not currently governed by HIPAA breach requirements.

By adopting this change, the FTC would be filling the gap left by HIPAA regulations and would assist in supporting the cross-governmental effort to empower patients with their health data. At the same time, this revised definition would ensure third-party application developers and the platforms that host those applications would be able to utilize the new regulatory requirements to their fullest extent, while better protecting individual privacy or health data security. Finally, this broader definition would give the FTC more jurisdiction to enforce the Rule.

Currently, only three breaches have been notified to the FTC and made public[9]. Yet, many more instances of individual health data being breached have occurred since the Rule was finalized. Most recently, Garmin had its internal servers compromised by a ransomware attack[10]. Under the current version of the Rule, Garmin is not required to report this breach since it is not a PHR vendor. In contrast, under the HIPAA Breach Notification Rule, there have been 575 notifications of a breach of 500 or more records since just August 2018 alone[11]. By enacting CHIME's proposed revision to the Rule, changing PHR to those non-HIPAA vendors storing EHI, Garmin would be subject to breach notification requirements due to its handling of information from users such as body weight, body height and heart rate – all data elements that are part of the USCDI.

2. What benefits has the Rule provided to consumers? What evidence supports the asserted benefits? What modifications, if any, should be made to the Rule to increase the benefits to consumers? How would these modifications affect the costs the Rule imposes on businesses, including small businesses?

Comment: As currently written, the Rule does not provide much benefit to consumers due to the lack of applicability to the real-world use of personal health information (PHI). With the Rule continuing to only govern PHR vendors and PHR-related entities, relatively few entities will find themselves covered under the Rule, while also remaining outside the purview of HIPAA. As previously noted, the significantly low number of reported breaches to the FTC related to the Rule signals either that entities handling health data don't believe they are covered as part of the Rule or that there is the lack of enforcement authority by the FTC to pursue these breaches. A strengthening of this rule and its applicable enforcement authority would provide consumers with more avenues to ensure and understand the safety of their health data.

The impact to businesses that appropriately handle consumer's personal health information would face no increased cost to their annual budgets given that this rule only requires notification due to health information being compromised through a breach. Similarly, covered entities are already required to notify breaches and are subject to the breach notification requirements contained within the HIPAA Law[12]. For those actors who inappropriately protect customer data, on average, an

[9] https://www.ftc.gov/system/files/documents/rules/health-breach-notification-rule/breach_notices_received_by_the_ftc.pdf
[10] https://www.zdnet.com/article/garmin-services-and-production-go-down-after-ransomware-attack/
[11] https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf
[12] https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html

IBM/Ponemon study found a data breach to cost $242 per stolen record[13], a cost that businesses will most likely incur whether they are required to report the breach to the FTC or not. Further expanding this rule will only help consumers be more informed about how their health information is handled and will largely leave businesses with no additional costs incurred.

3. What benefits, if any, has the Rule provided to businesses, including small businesses? What evidence supports the asserted benefits?

   Comment: The health information sector is currently booming within the U.S. economy and will only continue to grow as more patient health data is unlocked through the implementation of APIs. With more information available, and more patients looking to find, utilize and house that information, there will be more businesses looking to carve out market share. Businesses need to compete on trust and it is important that businesses that plan for, secure, and notify customers of appropriate actions related to health data security are not pushed to the side by those more interested in capturing a dedicated user base than in ensuring consumers are protected. A 2016 Rand study found that only 11% of consumers who were notified of a data breach stopped doing business with that organization[14]. With that in-mind, repeated reporting of data mishandling is crucial for businesses to be able to compete on the same playing field when it comes to protecting the consumer.

4. What modifications, if any, should be made to the Rule to account for changes in relevant technology, economic conditions, or laws? For example, as the healthcare industry adopts standardized application programming interfaces (''APIs'') to help individuals to access their electronic health information with smartphones and other mobile devices (as required by rules implementing the 21st Century Cures Act), will the number of entities subject to the Commission's HBN Rule increase?

   Comment: As previously stated, many of the third-party application developers targeted by ONC and CMS' 21st Century Cures Act Rules are not subject to the current FTC Breach Notification Rule, nor the HIPAA Breach Law. The aim of the ONC and CMS rules is to allow patients to have more access to and control of their health data. CHIME has remained steadfast in its support of this rule and the expansion of a patient's access to their health data. With greater patient access and movement of data, though, comes a greater responsibility placed on the applications and entities who handle the data. This increase in data handling also comes with the greater need for clarity on which privacy rule applies.

   In-terms of clarity of rule authority, as stated above, the current version of the Rule explicitly states PHR vendors and PHR-related entities are those governed by its requirements. In this new world of API-enabled patient access, does downloading your health data on a mobile telephone such as through Apple's Health Kit now cause Apple to be a PHR vendor or PHR-related entity? Similarly, does a product such as a mobile application like the much talked about contact tracing apps used to fight COVID-19 fall into the category of a PHR-related entity? Without further clarity provided by FTC on who is governed by the Rule, entities like the two previously outlined fall through the cracks and have no breach notification requirements. **With that in mind, we will again recommend the FTC change its governing authority for the Rule from PHR vendors and PHR-related entities to entities that handle EHI. If the FTC seeks more specificity related to what exact types of**

[13] https://www.ibm.com/security/data-breach

[14] https://www.rand.org/content/dam/rand/pubs/research_reports/RR1100/RR1187/RAND_RR1187.pdf

entities are required under the Rule, we recommend the FTC use the term "non-HIPAA covered Actors," with actors sharing the definition used in ONC and CMS' 21st Century Cures Act rules.

While also clarifying who is governed by the Rule, it is clear there needs to be clarity provided by the FTC on who is required to notify the FTC of a potential breach. For instance, if a "platform" such as an iPhone or an Android phone is compromised, causing for health data stored in a mobile application to be compromised, should the platform manager or the app developer be responsible for the breach notification? Without this clarity, it is possible neither entity may think it is responsible for notifying the FTC and thus no one will.

5. Does the Rule overlap or conflict with other federal, state, or local laws or regulations? If so, how?

   Comment: The Rule does not currently overlap or conflict with current regulation to the best of CHIME's knowledge. As it stands currently, we recommend the Rule be strengthened to further bring entities currently outside of other regulations into the alignment with their peers who also handle health information. By requiring all entities that handle EHI to be party to the Rule, then a hole in federal law will be filled.

Specific Questions

1. What evidence exists that the Rule has resulted in under-notification, overnotification, or an efficient level of notification?

   Comment: The lack of publicly reported breach notifications – three – indicates the Rule currently results in an under-notification of breaches.

2. Section 318.1 provides that the Rule does not apply to HIPAA-covered entities or to any other entity to the extent that it engages in activities as a business associate of a HIPAA-covered entity. Has this limitation helped to harmonize the Commission's HBN Rule with HHS's rule? Why or why not?

   Comment: Altering the Rule to have it correspond with HIPAA is key for filling the void left by HIPAA as it relates to non-covered entities. However, as currently outlined – with the Rule only applying to PHR vendors PHR related entities – the goal of ensuring widespread health data protection is left unmet.

3. Do the definitions set forth in § 318.2 of the Rule accomplish the Recovery Act's goal of advancing the use of health information technology while strengthening the privacy and security protections for health information?

   Comment: No, the definitions set forth do not accomplish the goal of strengthening privacy and security protections for health information. As stated above, the narrow definition of applicability to PHR vendors and PHR-related entities no longer accurately reflects the health technology and data handling environment as it exists today. With health data no longer sequestered in PHRs, it is crucial for privacy and security regulations to meet the information where it is, with patients' health data strung throughout multiple applications.

4. Should the definition of ''PHR identifiable health information'' in § 318.2(d) be modified in light of technological advances in methods of de-identification and re-identification? If so, how, consistent

with the Act's requirements? Should the definitions of ''PHR related entity'' in § 318.2(f), ''Third party service provider'' in § 318.2(h), or ''Vendor of personal health records'' in Section 318.2(j) be modified in light of changing technological and economic conditions, such as the proliferation of mobile health applications (''apps''), virtual assistants offering health services, and platforms' health tools? If so, how, consistent with the Act's requirements?

Comment: As stated above, the Rule should be modified to change the text of applicability from PHR vendors and PHR-related entities to instead contain language related to entities that handle EHI. By focusing on the type of data, as opposed to how the data is stored, ensures new technologies only now being introduced – or not even yet developed – will be captured by either HIPAA or this breach notification rule. This ensures privacy and security will be a cornerstone of health technology development and innovation now, as well as in the future. By changing the Rule to focus on content, as opposed to modality, it will bring consistency to the industry and ensure the Rule does not fall out of line with further regulatory developments from ONC and CMS on APIs and information blocking. Clarity is key and consistency is crucial when it comes to privacy and security regulations to ensure maximum compliance, and CHIME believes basing the Rule on EHI will provide those crucial pieces.

5. Section 318.4 sets out the timing requirements for notification. Are these requirements clear and appropriate? If not, how can they be improved, consistent with the Act's requirements?

   Comment: The timing requirements within the Rule continue to be appropriate. CHIME recommends the FTC monitor stakeholder feedback and propose, as well as update these requirements as needed over time.

6. Section 318.5 sets out the requirements for the method of notice of a breach. Are these requirements clear and appropriate? Do technological changes, such as the increased use of in app messaging, text messages, and platform messaging, warrant any changes to this section, consistent with the Act's requirements?

   Comment: The breach notification requirements are clear and appropriate. CHIME recommends the FTC monitor stakeholder feedback and propose, as well as update these requirements as needed over time.

7. Section 318.6 sets out the requirements for the content of notice of a breach. Are these requirements clear and appropriate? If not, how can they be improved, consistent with the Act's requirements?

   Comment: The content of the breach notifications is clear and appropriate. CHIME recommends the FTC monitor stakeholder feedback and propose, as well as update these requirements as needed over time.

8. What are the implications (if any) for enforcement of the Rule raised by direct-to-consumer technologies and services such as mobile health apps, virtual assistants, and platforms' health tools?

   Comment: Enforcement of the Rule on technologies and services such as mobile health apps, virtual assistants, and platforms' health tools will be vast and are crucial to protecting consumer health information. Consumers will be continuously inundated with new products and services

involving their health data. As has been shown with expanding markets of innovation, there can be a vacuum of new ideas and when that happens consumers are required to make decisions based on brand trust. This trust is built through advertising and often with data technology, it is built over privacy and security. Without a true way to hold these technology companies responsible for dangerous or unsafe data privacy practices, consumers will not ever be able to have the full picture of an entity when they make their decision.

The importance of providing this full picture of an application also extends to providers as well. As part of ONC's revised information blocking final rule, providers may:

> "Establish processes where they notify a patient, call to a patient's attention, or display in advance (as part of the app authorization process with certified API technology) whether the third-party developer of the app that the patient is about to authorize to receive their EHI has attested in the positive or negative as to whether the third party's privacy policy and practices (including security practices) meet certain "best practices" set by the market for privacy policies and practices.[15]"

It is imperative for providers to be able to view not only the "app developers'" privacy and security practices, but also to check to ensure the "app developer" has followed its own policies. The Rule and the FTC Breach Notification process is another opportunity for providers to inform their patients to ensure the safe handling of their data. Without modifying the Rule to ensure these "app developers" are included, providers will be able to provide their patients with only an incomplete picture of security and trust.

We appreciate the opportunity to comment and welcome the chance to help inform the critical work being done by the FTC with Breach Notification. We look forward to continuing to be a trusted stakeholder on addressing healthcare data and privacy issues as they continue to evolve and would like to engage further with the FTC as appropriate to discuss our comments and other key issues related to health data security. Should you have any questions about our letter, please contact Andrew Tomlinson, Director of Federal Affairs, at atomlinson@chimecentral.org.

Sincerely,

Russell P. Branzell, CHCIO, LCHIME
President and CEO CHIME

John Kravitz
Chair, CHIME Board of Trustees
CIO, Geisinger

[15] https://www.healthit.gov/sites/default/files/cures/2020-03/NPRMvsFinalRule.pdf